

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

APPLICANT(S): Kyung-Hee LEE, et al  
SERIAL NO.: not yet assigned  
FILED: herewith  
FOR: **AUTHENTICATION METHOD FOR FAST HANDOVER IN A  
WIRELESS LOCAL AREA NETWORK**  
DATED: October 9, 2003


Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**TRANSMITTAL OF PRIORITY DOCUMENTS**

Sir:

Enclosed is a certified copy of Korean Patent Appln. No.  
2002-62994 filed on October 15, 2002, from which priority is claimed under 35  
U.S.C. §119.

Respectfully submitted,

  
\_\_\_\_\_  
Paul J. Farrell, Esq.  
Reg. No. 33,494  
Attorney for Applicant(s)

**DILWORTH & BARRESE, LLP**  
**333 Earle Ovington Blvd.**  
**Uniondale, NY 11553**  
**(516) 228-8484**

---

**CERTIFICATION UNDER 37 C.F.R. 1.10**

I hereby certify that this New Application Transmittal and the documents referred to as enclosed therein are being deposited with the United States Postal Service in an envelope as "Express Mail Post Office to Addressee" Mail Label Number EV 333229182 US addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date listed below.

Dated: October 9, 2003

  
\_\_\_\_\_  
Jeff Kirshner



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원 번호 : 10-2002-0062994  
Application Number

출원 년 월 일 : 2002년 10월 15일  
Date of Application OCT 15, 2002

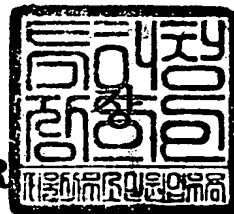
출원 인 : 삼성전자주식회사  
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.



2003      년      03      월      24      일

특      허      청

COMMISSIONER





## 【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0003
【제출일자】	2002. 10. 15
【국제특허분류】	H04K
【국제특허분류】	H04L
【발명의 명칭】	무선 근거리 네트워크에서 고속 핸드오버를 위한 인증방법
【발명의 영문명칭】	AUTHENTICATION METHOD FOR FAST HAND OVER IN WIRELESS LOCAL AREA NETWORK
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	1999-006038-0
【발명자】	
【성명의 국문표기】	이경희
【성명의 영문표기】	LEE, Kyung Hee
【주민등록번호】	710409-1648917
【우편번호】	442-725
【주소】	경기도 수원시 팔달구 영통동 벽적골 한신아파트 816동 1205호
【국적】	KR
【발명자】	
【성명의 국문표기】	성맹희
【성명의 영문표기】	SUNG, Maeng Hee
【주민등록번호】	660809-2037042
【우편번호】	121-837
【주소】	서울특별시 마포구 서교동 358-11
【국적】	KR
【심사청구】	청구

## 【취지】

특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인  
이건주 (인)

## 【수수료】

【기본출원료】	20	면	29,000	원
【가산출원료】	21	면	21,000	원
【우선권주장료】	0	건	0	원
【심사청구료】	31	항	1,101,000	원
【합계】	1,151,000			원

**【요약서】****【요약】**

본 발명은 무선 근거리 네트워크에서 이동 단말기의 고속 핸드오버를 위한 인증방법에 관한 것이다. 단말기가 최초로 액세스 포인트와 접속하고 초기 인증을 수행할 시, 단말기는 인증서버와 미리 공유하고 있는 비밀워드를 가지고 생성한 비밀키를 이용하여 인증서버로부터 암호 통신을 위한 세션키를 수신하며, 액세스 포인트는 인증서버와 미리 공유하고 있는 비밀키를 이용하여 인증서버로부터 세션키를 수신한다. 또한 단말기가 이전 액세스 포인트로부터 새로운 액세스 포인트로 핸드오버하고 재인증을 수행할 시, 단말기는 이전 인증시에 생성하여 인증서버와 공유하고 있는 인증정보를 가지고 생성한 비밀키를 이용하여 인증서버로부터 암호 통신을 위한 새로운 세션키를 수신하며, 새로운 액세스 포인트는 인증서버와 미리 공유하고 있는 비밀키를 이용하여 인증서버로부터 새로운 세션키를 수신한다. 이로써 핸드오버시에 새로운 액세스 포인트가 이전 액세스 포인트와 인증을 수행하거나 이전 인증에서 사용한 인증 정보를 안전하게 보관하여야 하는 부담없이 고속으로 단말기의 인증을 처리한다.

**【대표도】**

도 5

**【색인어】**

WLAN, wireless lan area network, handover, authentication,

**【명세서】****【발명의 명칭】**

무선 근거리 네트워크에서 고속 핸드오버를 위한 인증방법{AUTHENTICATION METHOD FOR FAST HAND OVER IN WIRELESS LOCAL AREA NETWORK}

**【도면의 간단한 설명】**

도 1은 종래 기술에 따른 무선 근거리 네트워크의 핸드오버 및 인증 절차를 나타낸 도면.

도 2는 본 발명에 따른 무선 근거리 네트워크(WLAN) 시스템의 일 예.

도 3은 인증 서버에서 단말기를 인증하는 동작을 나타낸 도면.

도 4는 본 발명에 따라 초기 인증을 수행하는 동작을 나타낸 메시지 흐름도.

도 5는 본 발명에 따라 재인증을 수행하는 동작을 나타낸 메시지 흐름도.

도 6은 본 발명에 따라 인증을 수행하는 이동 단말기의 동작을 나타낸 흐름도.

도 7은 본 발명에 따른 인증서버의 동작을 나타낸 흐름도.

도 8은 본 발명에 따른 액세스 포인트의 동작을 나타낸 흐름도.

**【발명의 상세한 설명】****【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <9>        본 발명은 무선 근거리 네트워크에 관한 것으로서, 특히 이동 단말기의 고속 핸드 오버를 위한 인증 방법에 관한 것이다.
- <10>       무선 근거리 네트워크(Wireless Local Area Network: WLAN)는 건물이나 학교 내부의 유선 근거리 네트워크(LAN)의 대안 내지는 확장판으로 구현된 유연성이 뛰어난 데이터 통신 시스템이다. 무선 근거리 네트워크는 무선 주파수(Radio Frequency: RF) 기술을 사용하여 최소한의 회선 연결만으로 무선으로 데이터를 주고받을 수 있다. 이와 같이 무선 근거리 네트워크는 간단한 설비만으로 사용자가 마음대로 이동하면서 데이터를 주고받을 수 있는 이른바 움직이는 네트워크를 가능하게 한다.
- <11>       무선 근거리 네트워크는 제한된 영역(이하 "셀(cell)"이라 한다.)을 서비스하는 적어도 하나의 무선 액세스 포인트(Access Point: AP)로 구성된다. 이러한 무선 근거리 네트워크에서 셀들간을 이동하는 사용자 단말기가 끊임없이(seamless) 통신을 계속하게 하는 것은 매우 중요하다. 이를 위하여 하나의 액세스 포인트(Access Point: AP)에서 다른 액세스 포인트로 통신에 대한 제어를 넘기는 절차를 핸드오버(Handover)라고 한다.
- IEEE(Institute of Electrical and Electronics Engineers)에서는 액세스 포인트들간의 통신 및 핸드오버를 위한 프로토콜(Inter-Access Point Protocol: IAPP)을 정의하고 있다.(ANSI/IEEE Std. 802.11, Aug. 1999, IEEE Std. 802.11f/D3, January 2002)

<12> 핸드오버를 위해서는 이동 단말기와 액세스 포인트들간에 많은 시그널링 메시지들을 상호 교환하여야 하며 이는 지연의 한 요인이 되며 통화품질에 큰 영향을 미친다. 특히 이동 단말기가 액세스 포인트에 접속할 때마다 새로운 네트워크 식별 주소, 즉 IP 주소를 할당받는 경우, 핸드오버시에 해당하는 액세스 라우터를 찾고 상기 할당된 주소를 홈 에이전트(Home Agent)에 등록하는 등 보다 많은 시그널링 절차가 필요하게 된다. 따라서 무선 통신 환경에서 핸드오버를 효율적으로 수행하기 위한 여러 가지 기술들이 연구되고 있다.

<13> 한편 무선 근거리 네트워크는 선로 작업등의 복잡한 작업없이 사용자가 간편하게 사용할 수 있지만, 반대로 허가받지 않은 사용자도 네트워크에 간단하게 접속할 수 있다는 단점이 있다. 액세스 포인트가 물리적으로 외부와 차단되어 있는 경우, 네트워크에 연결된 액세스 포인트는 자신의 영역으로 새롭게 진입하는 이동 단말기에 대해 인증 작업 없이 네트워크 접근을 허용하는 경우가 많다. 그러나 WLAN에서는 무선 신호의 특성상 신호 전달 영역을 제한하기가 어렵기 때문에, 사용자들의 네트워크 접근 권한에 대한 차별화 등의 부가 기능을 위해서는 단말기와 액세스 포인트간 상호 인증기능이 제공되어야 한다. 따라서 기업 등 보안이 중요시되는 조직에서 무선 근거리 네트워크를 사용하려면, 핸드오버에 의해 여러 액세스 포인트들을 거쳐 네트워크에 접근을 시도하는 단말기에 대해 상호 인증이 반드시 필요하다.

<14> IAPP에 따르면, 통신중인 단말기가 새로운 액세스 포인트에 접근하여 재접속(re-association)을 요구할 때, 상기 새로운 액세스 포인트는 상기 단말기와 새로운 인증 절차를 거치지 않고 인증 서버(Authentication Server)의 제어하에 이전 액세스 포인



트로부터 인증 및 보안 정보를 제공받는다. 하지만 이러한 경우 액세스 포인트들간에 메시지들을 교환하기 위해서도 인증은 필요하다.

<15> 도 1은 종래 기술에 따른 무선 근거리 네트워크의 핸드오버 및 인증 절차를 나타낸 것이다.

<16> 상기 도 1을 참조하면 이동 단말기(1)가 액세스 포인트1(2)의 서비스영역에서 액세스 포인트2(3)의 서비스영역으로 이동함에 따라 액세스 포인트2에게 재접속 요구(re-associate request)를 전달하면, (110) 액세스 포인트2(3)는 먼저 인증 서버(Authentication Server: AS)(4)에게 액세스 포인트1(2)과의 통신을 위한 보안 정보를 질의(Query)한다. (120) 인증 서버(4)로부터 상기 질의에 대한 응답을 수신하면(130) 액세스 포인트2(3)는 액세스 포인트1(2)에게 핸드오버를 요구하는 보안 블록(Security Block)을 전송한다. (140) 그러면 액세스 포인트1(2)은 단말기(1)와의 통신시에 사용한 인증 및 보안에 관련된 정보를 포함하는 보안 블록을 되돌려준다. (150) 그리고 액세스 포인트2(3)가 IAPP에 따라 자신의 동작 상태를 알리는 이동 요구(Move Request)를 액세스 포인트1(2)에게 전송하고(160) 그에 대한 응답을 수신하면, (170) 단말기(1)에게 재접속이 완료되었음을 알리고 통신을 개시한다. (180)

<17> 상기와 같이 동작하는 무선 근거리 네트워크의 핸드오버 방식에 있어서, 액세스 포인트들간 인증을 위한 방식으로써 현재 IPSec(Internet Protocol Security) 표준이 사용되고 있다. 상기 IPSec은 가상 사설 네트워크를 구현하고 원격 사용자가 사설 네트워크를 액세스하는데 특히 유용할 수 있다. 반면 IPSec를 실행하기 위해서는 액세스 포인트의 구조가 복잡해질 뿐만 아니라 액세스 포인트간 인증을 위한 공개키(public key) 기반 구조가 필요하다는 문제점이 발생한다.

<18> 액세스 포인트들이 액세스 포인트간 인증을 위한 비밀워드(security word)를 미리 공유하는 경우 공개키 기반 구조가 필요하지 않을 수 있으나, 이때는 액세스 포인트들의 개수가 많아질수록 상기 비밀워드를 유지 관리하기 위한 부담이 증가하게 된다는 다른 문제점이 발생한다. 즉, 단말기가  $n$ 개의 액세스 포인트들을 경유한 경우 각 액세스 포인트는  $n-1$ 개의 비밀워드들을 유지하여야 한다. 게다가 이러한 경우 네트워크상의 인증 서버는 액세스 포인트들간 데이터 전송 시 사용되는 각각의 IPSec 보안 연결들(security associations)을 관리해야 한다.

<19> 특히 핸드오버 시 상기 인증 방식은 또 다른 보안상의 문제점을 야기하는데, 즉 이전 액세스 포인트와 단말기 사이에 사용된 인증 및 보안 정보가 핸드오버 이후에도 계속 사용된다는 것이다. 이에 따라서 단말기가 현재 통신하고 있는 액세스 포인트와 안전하게 계속 통신하기 위해서는 이전 액세스 포인트들 모두가 여전히 안전해야 한다. 즉, 그만큼 보안이 노출될 가능성이 컸다는 문제점이 있었다.

#### 【발명이 이루고자 하는 기술적 과제】

<20> 따라서 상기한 바와 같이 동작되는 종래 기술의 문제점을 해결하기 위하여 창안된 본 발명의 목적은 무선 근거리네트워크에서 이동 단말기와 액세스 포인트간 암호 통신을 위한 방법을 제공하는 것이다.

<21> 본 발명의 다른 목적은 무선 근거리네트워크에서 이동 단말기의 인증을 처리하는 방법을 제공하는 것이다.

- <22>      본 발명의 다른 목적은 무선 근거리네트워크에서 액세스 포인트들간 핸드오버시 이동 단말기의 인증을 처리하는 방법을 제공하는 것이다.
- <23>      본 발명의 또 다른 목적은 무선 근거리네트워크에서 액세스 포인트들간 통신없이 이동 단말기를 고속으로 인증하는 방법을 제공하는 것이다.
- <24>      상기한 바와 같은 목적을 달성하기 위하여 창안된 본 발명의 실시예는, 단말기와 무선 접속을 설정하는 적어도 2개의 액세스 포인트들과 상기 단말기를 인증하는 인증서버를 포함하는 무선 근거리 네트워크에서 상기 단말기를 인증하는 방법에 있어서,
- <25>      단말기가 제1 액세스 포인트와 접속하고 초기 인증을 수행할 시, 단말기가 상기 인증서버와 미리 공유하고 있는 비밀워드를 가지고 생성한 제1 비밀키를 이용하여 상기 인증서버로부터 암호 통신을 위한 제1 세션키를 수신하고, 상기 제1 액세스 포인트가 상기 인증서버와 미리 공유하고 있는 제2 비밀키를 이용하여 상기 인증서버로부터 상기 제1 세션키를 수신하는 제1 과정과,
- <26>      상기 단말기가 상기 제1 액세스 포인트로부터 제2 액세스 포인트로 핸드오버하고 재인증을 수행할 시, 상기 단말기가 이전 인증시에 생성하여 상기 인증서버와 공유하고 있는 인증정보를 가지고 생성한 제3 비밀키를 이용하여 상기 인증서버로부터 암호 통신을 위한 제2 세션키를 수신하고, 상기 제2 액세스 포인트가 상기 인증서버와 미리 공유하고 있는 상기 제2 비밀키를 이용하여 상기 인증서버로부터 상기 제2 세션키를 수신하는 제2 과정을 포함한다.

## 【발명의 구성 및 작용】

- <27> 이하 첨부된 도면을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.
- <28> 도 2는 본 발명에 따른 무선 근거리 네트워크(WLAN) 시스템의 일 예를 도시한 것이다.
- <29> 상기 도 2를 참조하면, 무선 근거리 네트워크(WLAN)(10)는 교환기들(Switches)(12,14,16)과, 인터넷이나 공중 교환 전화 네트워크(publish switched telephone network: PSTN)와 같은 외부 네트워크(20)에 연결되기 위한 게이트웨이(18)를 가진다. 상기 교환기들(12,14,16)은 각각 무선 이동 단말기들(34,36)과 무선 접속이 가능한 액세스 포인트들(24,26,28,30,32)을 상기 외부 네트워크(20)로 연결한다.
- <30> 이동 단말기들(34,36)은 전송하고자 하는 데이터를 액세스 포인트와의 인증 절차에서 획득한 세션 키를 가지고 암호화하며, 액세스 포인트들(24,26,28,30,32)로부터 수신된 데이터를 상기 세션 키를 가지고 복호한다. 세션 키는 이동 단말기와 액세스 포인트 간의 관계에 대하여 유일하며 이로써 안전한 암호 통신이 가능해진다. 이때 인증 서버(20)는 스위치들(12,14,24)을 통해 액세스 포인트에 접속하고 상기 이동 단말기들(34,36)의 인증을 처리한다.

- <31> 도 3은 인증 서버에서 단말기를 인증하는 동작을 나타낸 것이다.
- <32> 상기 도 3을 참조하면, 홈 인증서버(Home AS: H-AS)(42)는 클라이언트의 상호 인증을 위해 자신에게 소속된 단말기들(50,52)이 제공하는 신임장(credential)을 검증할 수 있다. 홈 도메인(home domain)에서 네트워크에 접근하는 단말기(52)는 해당하는 액세스 포인트(48)를 통해 홈 인증서버(42)에 접속하며, 홈 인증서버 (42)로부터 직접 인증받을 수 있다.
- <33> 외부 인증서버(Foreign AS: F-AS)(40)는 클라이언트가 방문 도메인(visited domain)에서 네트워크에 접근할 때 먼저 접속되는 인증 서버이다. 외부 인증서버(40)는 접속을 요청한 단말기(50)가 자신의 도메인에 속하지 않으면 단말기 인증을 위해서 상기 단말기(50)가 소속된 홈 인증서버(42)에게 인증을 요청한다. 이를 위해서 홈 인증서버(42)와 외부 인증서버(40) 간에 보안접속(Security Association: SA)이 존재하며 이를 SA2라 표기하였다.
- <34> 단말기(50)가 방문 도메인에서 액세스 포인트(44) 또는 액세스 포인트(46)에 접속하면 액세스 포인트들(44,46)은 단말기(50)로부터 제공받은 신임장을 외부 인증서버(40)에 넘겨주며, 외부 인증서버(40)는 SA2를 통해 받은 인증 결과를 액세스 포인트들(44,46)을 통해 단말기(50)에 알려준다. 이때 외부 인증서버(40)와 액세스 포인트들(44,46)간에 서로를 인증하기 위한 보안 접속 SA1과, 또한 단말기(50)의 신임장이 홈 인증서버(42)에 전달된 후 단말기(50)와 홈 인증서버(42)간에 상호 인증을 위한 보안 접속 SA1이 필요하다.

- <35> 액세스 포인트들은 자신으로부터 방사되는 무선 신호의 수신 세기에 의해 정해지는 소정의 서비스영역을 가지며, 이는 셀(cell)이라 불리운다. 셀들은 서로간에 부분적으로 중첩될 수 있으며 이 중첩된 영역에서 핸드오버(Handover)가 발생한다. 무선 근거리 네트워크에서 핸드오버가 이루어지는 원리에 대해 설명하면 다음과 같다.
- <36> 모든 액세스 포인트들은 정기적으로 초당 10개의 비콘 속도(beacon rate)로 비콘 신호를 방송(broadcast)한다. 단말기는 인접한 액세스 포인트들로부터 수신되는 비콘 신호들의 신호세기들을 비교하며 가장 강한 신호세기를 가지는 액세스 포인트와 접속(association)한다. 그러면 상기 액세스 포인트는 자신의 식별자 (Identifier: ID) 및 통신 가능한 전송율(data rate) 등에 관한 정보를 단말기에 전송하고 통신을 시작한다.
- <37> 상대방과 통신하면서 움직이는 단말기는 현재 통신하고 있는 액세스 포인트로부터의 비콘 신호가 약해지면 소정 임계값만큼 더 강한 다른 비콘 신호가 있는지 검사한다. 만일 더 강한 비콘 신호가 존재하면, 그 비콘 신호를 송출하는 새로운 액세스 포인트로 핸드오버하기 위해서 단말기는 상기 새로운 액세스 포인트에게 재접속 요구(re-association request)를 보낸다. 그러면 상기 새로운 액세스 포인트는 필요한 정보를 단말기에게 전송하고 통신을 시작한다.
- <38> 단말기가 여러 지역을 돌아다니는(roaming) 무선 환경의 경우, 통신의 끊김없는(seamless) 연속성을 보장하기 위해서는 2 계층 또는 3 계층의 관리 신호(management signals)와 네트워크와 단말기간 상호인증에 필요한 시그널링 부하(signaling load)를 줄이는 것이 필요하다. 특히 본 발명은 네트워크와 단말기간 접속(association)이 이루어진 이후 인증의 수행시에 필요한 시그널링 부하의 감소에 관련된다.
- <39> 먼저 본 발명에 필요한 인증정보들에 대해 설명하면 하기와 같다.

- <40>        - S : 단말기와 인증서버간에 공유되는 비밀워드.
- <41>        - E\_k : 단말기와 인증서버간에 k를 비밀키(private key)로 사용하는 대칭 키 암호 알고리즘.
- <42>        - E\_kAP : 액세스 포인트와 인증서버간에 공유되는 비밀키 kAP를 사용하는 대칭 키 암호 알고리즘.
- <43>        - H(.) : 해쉬 함수(Hash Function)
- <44>        - Sk : 단말기와 액세스 포인트간에 암호 통신을 위해 사용되는 세션 키.
- <45>        - TID : 단말기의 임시 식별자(Temporary Identifier: TID).
- <46>        - PID : 단말기의 영구 식별자(permanent Identifier: PID).
- <47>        - nonce : 단말기에서 생성하는 난수(random number).
- <48>        하기에서 본 발명에 따른 인증동작을 설명함에 있어서, 단말기가 최초로 통신을 개시할 때 첫 번째 액세스 포인트와 수행하는 인증을 초기 인증( $i=0$ , 여기서  $i$ 는 인증을 식별하는 인덱스)이라 하고 이후 핸드오버에 의해 접속하는 액세스 포인트들과 수행하는 인증을 재인증( $i \neq 0$ )이라 하기로 한다. 이러한 경우 상기 인증절차에 필요한 정보들 중 E\_kAP와 H(.)와 PID는 변화하지 않지만, E\_k와 Sk와 TID와 nonce는 매 인증시마다 변화하게 된다.
- <49>        또한 하기에서 본 발명을 설명함에 있어서 인증정보의 구체적인 예를 들어 설명할 것이나, 실제로 본 발명은 이전 인증시에 사용한 인증정보를 이용하여 재인증을 수행하는 것으로서, 인증정보의 종류나 이름에 의해 제한되는 것이 아님은 물론이다.

- <50> 도 4는 본 발명에 따라 초기 인증을 수행하는 동작을 나타낸 메시지 흐름도이다. 하기에서 인증서버는 단말기가 소속된 홈 인증서버로서, 만일 단말기가 방문 도메인에 있다면 외부 인증서버를 통해 인증 절차를 수행하게 된다. 또한 인증서버와 그에 접속하는 액세스 포인트들은 상호간의 통신을 위한 비밀키  $k_{AP}$ 를 공유한다.
- <51> 단말기(MN)는 전원을 켜 후 최초로 감지된 액세스 포인트 AP1과 무선 접속을 설정하고 인증서버(AS)와 사전 인증을 수행한다. 여기서의 사전 인증은 단말기가 인증서버와 통신을 수행하는데 필요한 것으로서, 사용자에게 의해 입력된 패스워드, 사용자의 생체정보(홍채 또는 지문 등), 스마트 카드(Smart Card) 등을 이용하여 이루어질 수 있다. 이러한 사전 인증은 알려진 기존의 인증 프로토콜에 따라 이루어질 수 있다. 사전 인증에 의해 단말기와 인증서버는 비밀워드 S를 공유하게 되며, 단말기와 인증서버는 각각 상기 비밀워드 S를 입력으로 하는 해쉬함수 H를 이용해서 상호간 메시지 교환에 이용되는 비밀키  $k_0 = H(S)$ 를 얻는다.
- <52> 사전 인증이 완료되면, 단말기는 다음 인증 요청시 사용하게 될 인증정보, 즉 임시 식별자 TID1, 패스워드 Y1 및 난수 nonce1을 생성하고, 상기 생성된 인증정보를 상기 비밀키  $k_0$ 을 이용해서 암호화하여 암호화 메시지  $B_0 = E_{k_0}(PID, TID1, Y1, nonce1)$ 을 생성한다. 상기 암호화 메시지  $B_0$ 은 인증을 요청하기 위하여, 액세스 포인트 AP1을 통해서 인증서버에게 전송된다. 이때 상기 단말기의 영구 식별자 PID가 상기 암호화 메시지  $B_0$ 과 함께 전송될 수 있다.(200)
- <53> 인증서버는 상기 암호화 메시지  $B_0$ 을 수신한 후 상기 비밀키  $k_0$ 을 이용해서 복호하고, 상기 복호결과 얻은 상기 인증정보 중 임시 식별자 TID1과 패스워드 Y1을 다음 인증



시에 사용하기 위하여 단말기 관련 데이터 베이스에 보관한다. 그리고 인증서버는 상기 단말기의 데이터 패킷 암호화에 사용될 세션키  $Sk_0$ 을 생성한 후, 상기 생성한 세션키  $Sk_0$ 과 상기 암호화 메시지 B0에서 얻은 난수  $nonce_1$ 을 상기 비밀키  $k_0$ 으로 암호화하여 암호화 메시지  $A_0 = E_{k_0}(nonce_1, Sk_0)$ 을 생성한다. 상기 암호화 메시지  $A_0$ 은 단말기의 인증을 허가하고 상기 세션키  $Sk_0$ 을 전달하기 위한 것이므로, 인증 절차를 단축하고자 하는 경우 상기 난수  $nonce_1$ 은 상기 암호화 메시지  $A_0$ 에 포함되지 않을 수 있다.

<54> 또한 인증서버는 상기 생성한 세션키  $Sk_0$ 과 상기 암호화 메시지 B0에서 얻은 난수  $nonce_1$  및 단말기의 영구 식별자 PID를 액세스 포인트들과의 통신에 사용되는 비밀키  $k_{AP}$ 를 사용하여 암호화하여 암호화 메시지  $P_0 = E_{k_{AP}}(Sk_0, nonce_1, PID)$ 을 생성한다. 여기서 상기 난수  $nonce_1$  및 상기 영구 식별자 PID는 상기 암호화 메시지  $P_0$ 에 포함되지 않을 수 있다. 상기 암호화 메시지  $P_0$ 은 액세스 포인트에게 단말기의 인증이 허가되었음을 알리고 상기 세션키  $Sk_0$ 을 전달하기 위한 것이며, 상기 비밀키  $k_{AP}$ 는 인증서버에 접속하는 액세스 포인트들이 필수적으로 이미 가지고 있는 것이다. 상기 암호화 메시지들  $A_0$ 과  $P_0$ 은 액세스 포인트 AP1로 전송된다.(210)

<55> 액세스 포인트 AP1은 인증서버와 공유하고 있는 비밀키  $k_{AP}$ 를 이용해서 상기 암호화 메시지  $P_0$ 을 복호하고, 상기 복호결과 얻은 단말기의 영구 식별자 PID와 세션키  $Sk_0$ 을 저장한다. 그리고 상기 암호화 메시지  $A_0$ 을 단말기에게 바이패스한다.(220)

<56> 단말기는 상기 비밀키  $k_0$ 을 이용해서 상기 암호화 메시지  $A_0$ 을 복호하여 난수  $nonce_1$ 과 세션키  $Sk_0$ 을 얻는다. 만일 상기 복호결과 얻은 난수  $nonce_1$ 이 상기 과정(200)에서 생성한 난수와 동일하면, 단말기는 상기 복호결과 얻은 세션키  $Sk_0$ 이 정확한 것으

로 판단하고 상기 세션키  $Sk_0$ 을 이용하여 암호 통신을 수행한다. 인증 절차를 단축하고자 하는 경우 단말기는 난수를 비교하지 않고 상기 세션키  $Sk_0$ 을 사용한다.(230)

<57> 도 5는 단말기가 초기 접속 이후 핸드오버에 의해 새로운 액세스 포인트에 재접속을 시도하는 경우 본 발명에 따라 재인증을 수행하는 동작을 나타낸 메시지 흐름도이다. 마찬가지로 단말기는 홈 도메인에서 홈 인증서버와 직접 인증 절차를 수행하는 것으로 하며, 또한 인증서버와 그에 접속하는 액세스 포인트들은 상호간의 통신을 위한 비밀키  $k_{AP}$ 를 공유한다.

<58> 먼저 단말기(MN)는 핸드오버에 의해 2번째 액세스 포인트 AP2에 접속하면 이전 액세스 포인트 A1과의 인증시에 생성한 패스워드  $Y_1$ 을 해쉬함수의 입력으로 하여 인증서버와의 메시지 교환에 이용되는 비밀키  $k_1=H(Y_1)$ 를 얻는다. 그리고 단말기는 다음 인증 요청시 사용하게 될 인증정보, 즉 임시 식별자 TID2, 패스워드  $Y_2$  및 난수 nonce2를 생성한 후, 상기 인증정보를 이전 인증시에 생성한 임시 식별자 TID1과 함께 상기 비밀키  $k_1$ 을 이용해서 암호화하여 암호화 메시지  $B_1 = E_{k_0}(TID1, TID2, Y_2, nonce2)$ 을 생성한다. 상기 암호화 메시지 B1은 상기 임시 식별자 TID1과 함께 액세스 포인트 AP2를 통해서 인증서버에게 전송된다. 이때 암호화되지 않은 형태의 상기 이전 임시 식별자 TID1이 상기 암호화 메시지 B1과 함께 전송될 수 있다.(240)

<59> 인증서버는 상기 암호화 메시지 B1을 수신한 후, 이전 인증시에 수신된 패스워드  $Y_1$ 을 해쉬함수의 입력으로 하여 단말기와의 메시지 교환에 이용되는 비밀키  $k_1=H(Y_1)$ 를 얻는다. 그리고 인증서버는 상기 비밀키  $k_1$ 을 이용해서 상기 암호화 메시지 B1을 복호화

여 얻은 인증정보 중 임시 식별자 TID2와 패스워드 Y2를 단말기 관련 데이터 베이스에 보관한다.

<60> 그리고 나면 인증서버는 상기 단말기의 데이터 패킷 암호화에 사용될 세션키 Sk1을 생성한 후, 상기 생성한 세션키 Sk1과 상기 암호화 메시지 B1에서 얻은 난수 nonce2를 상기 비밀키 k1로 암호화하여 암호화 메시지  $A1 = E_{k1}(\text{nonce1}, \text{Sk1})$ 을 생성한다. 이때 상기 암호화 메시지 A1은 상기 난수 nonce2를 포함하지 않을 수 있다. 또한 인증서버는 상기 생성한 세션키 Sk1과 상기 암호화 메시지 B0에서 얻은 난수 nonce2 및 이전 임시 식별자 TID1을 액세스 포인트들과의 통신에 사용되는 비밀키  $k_{AP}$ 를 사용하여 암호화하여 암호화 메시지  $P1 = E_{k_{AP}}(\text{Sk1}, \text{nonce2}, \text{TID1})$ 을 생성한다. 다른 경우 상기 암호화 메시지 P1은 상기 난수 nonce2와 상기 이전 임시 식별자 TID1을 포함하지 않는다. 상기 암호화 메시지들 A1과 P1은 액세스 포인트 AP2로 전송된다.(250)

<61> 액세스 포인트 AP2는 인증서버와 공유하고 있는 상기 비밀키  $k_{AP}$ 를 이용해서 상기 암호화 메시지 P1을 복호하고, 상기 복호결과 얻은 단말기의 임시 식별자 TID2와 세션키 Sk1을 저장한다. 그리고 상기 암호화 메시지 A1을 단말기에게 바이패스한다.(260)

<62> 단말기는 상기 비밀키 k1을 이용해서 상기 암호화 메시지 A1을 복호하여 난수 nonce2와 세션키 Sk1을 얻는다. 만일 상기 복호결과 얻은 난수 nonce2가 상기 과정(240)에서 생성한 난수와 동일하면, 단말기는 상기 복호결과 얻은 세션키 Sk1이 정확한 것으로 판단하고 상기 세션키 Sk1을 이용하여 암호 통신을 수행한다. 인증 절차를 단축하고자 하는 경우 단말기는 난수들을 비교하지 않고 상기 세션키 Sk1을 사용한다.(270)

<63> 이후 단말기가 3번째, 4번째 액세스 포인트들로 계속해서 핸드오버하는 경우에도 마찬가지로 이상에서 설명한 바와 같은 절차를 통해 인증이 이루어진다. 이로써 액세스

포인트들은 다른 액세스 포인트와 인증을 수행해야 하는 부담 없이 단말기와의 데이터 통신에 필요한 세션키를 얻는다.

<64> 도 6은 본 발명에 따라 인증을 수행하는 이동 단말기의 동작을 나타낸 흐름도이고, 도 7은 인증서버의 동작을 나타낸 흐름도이며, 도 8은 액세스 포인트의 동작을 나타낸 흐름도이다. 이하 상기 도 6 내지 도 8을 참조하여 본 발명에 따른 각 노드에서의 동작을 상세히 설명하기로 한다.

<65> 상기 도 6을 참조하면, 최초로 액세스 포인트와 접속을 설정한 경우, (300) 단말기는 알려진 인증 프로토콜에 따라 사전 인증을 수행하여 인증서버와의 사이에 공유되는 비밀워드 S를 얻는다. (305) 그러면 상기 비밀워드 S를 이용하여 해쉬함수의 출력인 비밀키  $k_0 = H(S)$ 를 계산하고, (310) 다음 인증 요청시 사용하기 위한 인증정보, 즉 임시 식별자 TID1과 패스워드 Y1과 난수 nonce1을 생성한다. (315) 여기서 상기 생성된 인증정보는 다음 인증에서 사용되기 위하여 저장된다.

<66> 상기 임시 식별자 TID1, 패스워드 Y1, 난수 nonce1은 상기 단말기의 영구 식별자 PID와 함께 상기 비밀키  $k_0$ 을 가지고 제1 암호문 B0으로 암호화된다. (320) 그러면 단말기는 상기 제1 암호문 B0을 상기 접속을 설정한 액세스 포인트를 통해 인증서버로 전송한다. (325)

<67> 이후 상기 액세스 포인트를 통해 상기 인증서버로부터 제2 암호문 A0이 수신되면 (330) 단말기는 상기 비밀키  $k_0$ 을 가지고 상기 제2 암호문 A0을 복호하여 난수 nonce1과 세션키  $Sk_0$ 을 검출한다. (335) 상기 검출된 난수 nonce1이 상기 과정(315)에서 생성한 난수 nonce1과 동일하면, 단말기는 상기 액세스 포인트로 전송하고자 하는 데이터를 상기

세션키  $Sk_0$ 으로 암호화하고 상기 액세스 포인트로부터 수신된 데이터를 상기 세션키  $Sk_0$ 으로 복호한다.(340)

<68> 한편 단말기가 이전  $(i-1)$ 번째 액세스 포인트로부터 새로운  $i$ 번째 액세스 포인트로 핸드오버한 경우,(300) 단말기는 이전 인증시에 생성하여 저장한 이전 패스워드  $Y(i)$ 를 이용하여 해쉬함수의 출력인 비밀키  $k(i)=H(Y(i))$ 를 계산하고,(350) 다시 다음 인증 요청시 사용하기 위한 인증정보, 즉 임시 식별자  $TID(i+1)$ 과 패스워드  $Y(i+1)$ 와 난수  $nonce(i+1)$ 를 생성한다.(355) 마찬가지로 상기 생성된 인증정보는 다음 인증에서 사용되기 위하여 저장된다.

<69> 상기 임시 식별자  $TID(i+1)$ , 패스워드  $Y(i+1)$ , 난수  $nonce(i+1)$ 는 이전 인증시에 생성하여 저장한 임시 식별자  $TID(i)$ 와 함께 상기 비밀키  $k(i)$ 를 가지고 제1 암호문  $B(i)$ 로 암호화된다.(360) 그러면 단말기는 상기 제1 암호문  $B(i)$ 를 상기 새로운 액세스 포인트를 통해 인증서버로 전송한다.(365)

<70> 이후 상기 새로운 액세스 포인트를 통해 상기 인증서버로부터 제2 암호문  $A(i)$ 가 수신되면(370) 단말기는 상기 비밀키  $k(i)$ 를 가지고 상기 제2 암호문  $A(i)$ 를 복호하여 난수  $nonce(i+1)$ 와 세션키  $Sk(i)$ 를 검출한다.(375) 상기 검출된 난수  $nonce(i+1)$ 가 상기 과정(355)에서 생성한 난수  $nonce(i+1)$ 와 동일하면, 단말기는 상기 새로운 액세스 포인트로 전송하고자 하는 데이터를 상기 세션키  $Sk(i)$ 으로 암호화하고 상기 새로운 액세스 포인트로부터 수신된 데이터를 상기 세션키  $Sk(i)$ 으로 복호한다.(380)

<71> 상기 도 7을 참조하면, 과정(400)에서 단말기가 최초로 액세스 포인트와 접속을 설정한 경우, 인증서버는 알려진 인증 프로토콜에 따라 사전 인증을 수행하여 비밀워드  $S$ 를 얻고(405) 상기 비밀워드  $S$ 를 이용하여 해쉬함수의 출력인 비밀키  $k_0=H(S)$ 를 계산한

다.(410) 이후 상기 액세스 포인트를 통해 상기 단말기로부터 제1 암호문 B0이 수신되면 (415) 인증서버는 상기 비밀키 k0을 가지고 상기 제1 암호문을 복호하여 상기 단말기의 영구 식별자 PID, 임시 식별자 TID1, 패스워드 Y1, 난수 nonce1을 검출한다.(420) 상기 임시 식별자 TID1과 상기 패스워드 Y1은 다음 인증시에 사용될 수 있도록 단말기 데이터 베이스에 저장된다.(425)

<72> 그러면 인증서버는 상기 단말기의 데이터 통신을 위해 사용될 세션키 Sk0을 생성하고(430), 상기 생성된 세션키 Sk0을 상기 검출된 난수 nonce1과 함께 상기 비밀키 k0을 가지고 암호화하여 제2 암호문 A0을 생성하며, 또한 상기 생성된 세션키 Sk0을 상기 검출된 난수 nonce1 및 상기 단말기의 영구 식별자 PID와 함께 액세스 포인트와의 통신을 위해 미리 저장하고 있던 비밀키 k<sub>AP</sub>를 가지고 암호화하여 제3 암호문 P0을 생성한다.(435) 상기 제2 암호문 A0과 상기 제3 암호문 P0은 상기 액세스 포인트로 전송된다.(440)

<73> 한편 과정(400)에서 단말기가 이전 (i-1)번째 액세스 포인트로부터 새로운 i번째 액세스 포인트로 핸드오버한 경우, 인증서버는 단말기로부터 이전 임시 식별자 TID(i)와 함께 제1 암호문 B(i)를 수신한다.(450) 그러면 인증서버는 상기 이전 임시 식별자 TID(i)을 가지고 단말기 데이터베이스를 검색하여 해당하는 이전 패스워드 Y(i)를 얻고 (455) 상기 이전 패스워드 Y(i)를 이용하여 해쉬함수의 출력인 비밀키 k(i)=H(Y(i))를 계산한다.(460) 상기 비밀키 k(i)에 의해 상기 제1 암호문 B(i)를 복호하여 이전 임시 식별자 TID(i)와 임시 식별자 TID(i+1)과 패스워드 Y(i+1)와 난수 nonce(i+1)을 검출한다.(465) 상기 검출된 임시 식별자 TID(i+1)과 상기 패스워드 Y(i+1)는 다음 인증시에 사용될 수 있도록 단말기 데이터베이스에 저장된다.(470)

<74> 이후 인증서버는 상기 단말기의 데이터 통신을 위해 사용될 세션키  $Sk(i)$ 을 생성하고(475), 상기 생성된 세션키  $Sk(i+1)$ 을 상기 검출된 난수  $nonce(i+1)$ 와 함께 상기 비밀키  $k(i)$ 를 가지고 암호화하여 제2 암호문  $A(i)$ 를 생성하며, 또한 상기 생성된 세션키  $Sk(i)$ 을 상기 검출된 난수  $nonce(i+1)$  및 상기 이전 임시 식별자  $TID(i)$ 와 함께 액세스 포인트와의 통신을 위해 미리 저장하고 있던 비밀키  $k_{AP}$ 를 가지고 암호화하여 제3 암호문  $P(i)$ 를 생성한다.(480) 상기 제2 암호문  $A(i)$ 와 상기 제3 암호문  $P(i)$ 는 상기 새로운 액세스 포인트로 전송된다.(485)

<75> 상기 도 8을 참조하면, 과정(500)에서 단말기가 최초로 액세스 포인트와 접속을 설정한 경우, 상기 액세스 포인트는 상기 단말기로부터 제1 암호문  $B_0$ 을 수신하고(505) 상기 수신된 제1 암호문  $B_0$ 을 인증서버로 전달한다.(510) 이후 상기 인증서버로부터 제2 암호문  $A_0$  및 제3 암호문  $P_0$ 이 수신되면(515) 상기 제3 암호문  $P_0$ 을 인증서버와의 통신을 위해 미리 저장하고 있던 비밀키  $k_{AP}$ 를 가지고 복호하여 세션키  $Sk_0$ , 난수  $nonce_1$ , 영구 식별자  $PID$ 를 검출한다.(520)

<76> 상기 검출된 세션키  $Sk_0$ 과 상기 영구 식별자  $PID$ 는 데이터 통신을 위해 사용될 수 있도록 저장된다.(525) 상기 액세스 포인트는 제2 암호문을 상기 단말기에게 전달한 후(530) 상기 단말기에게 전송하고자 하는 데이터를 상기 세션키  $Sk_0$ 으로 암호화하고 상기 단말기로부터 수신된 데이터를 상기 세션키  $Sk_0$ 으로 복호한다.(535)

<77> 한편 과정(500)에서 단말기가 이전  $(i-1)$ 번째 액세스 포인트로부터 새로운  $i$ 번째 액세스 포인트로 핸드오버한 경우, 상기 새로운 액세스 포인트는 상기 단말기로부터 이전 임시 식별자  $TID(i)$ 와 함께 제1 암호문  $B(i)$ 를 수신한다.(540) 상기 이전 임시 식별자  $TID(i)$ 는 상기 새로운 액세스 포인트에서 저장되고 상기 제1 암호문  $B(i)$ 와 함께 인

증서버로 전달된다.(545) 이후 상기 인증서버로부터 제2 암호문  $A(i)$  및 제3 암호문  $P(i)$ 가 수신되면(550) 상기 제3 암호문  $P(i)$ 를 인증서버와의 통신을 위해 미리 저장하고 있던 비밀키  $k_{AP}$ 를 가지고 복호하여 세션키  $Sk(i)$ , 난수  $nonce(i+1)$ , 임시 식별자  $TID(i+1)$ 를 검출한다.(555)

<78>       상기 검출된 세션키  $Sk(i)$ 와 상기 임시 식별자  $TID(i+1)$ 는 데이터 통신을 위해 사용될 수 있도록 저장된다.(560) 상기 새로운 액세스 포인트는 상기 제2 암호문을 상기 단말기에게 전달한 후(570) 상기 단말기에게 전송하고자 하는 데이터를 상기 세션키  $Sk(i)$ 으로 암호화하고 상기 단말기로부터 수신된 데이터를 상기 세션키  $Sk(i)$ 으로 복호한다.(575)

<79>       한편 본 발명의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되지 않으며, 후술되는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

### 【발명의 효과】

<80>       이상에서 상세히 설명한 바와 같이 동작하는 본 발명에 있어서, 개시되는 발명중 대표적인 것에 의하여 얻어지는 효과를 간단히 설명하면 다음과 같다.

<81>       무선 근거리 네트워크에서 단말기가 핸드오버에 의해 액세스 포인트를 바꾸면서 이동할 때 상호 인증 기능을 간단하고 빠르게 처리하여 단말기와 액세스 포인트간 비밀 통



신을 수행할 수 있는 키를 제공한다. 또한 핸드오버 이전과 이후 단말기가 이전에 통신한 액세스 포인트와 현재 통신하고 있는 액세스 포인트 사이의 보안 접속(security association)이 독립적이기 때문에 단말기가 이동 후 이전 액세스 포인트들 중 어느 하나가 공격당하더라도 현재 통신하는 세션에 대해서 안전성을 보장한다. 이 때문에 액세스 포인트간 보안 접속이 필요하지 않으며 이는 각 세션의 보안 정보에 대한 안전성을 높이는 효과를 보인다.

<82>        게다가 단말기가 이동 후 액세스 포인트를 통해서 상호 인증 시 필요한한 메시지들을 상호 교환함으로써 인증 시 필요한 시그널링의 양이 효과적으로 감소되며, 단말기가 액세스 포인트간을 이동 후 인증 요청 시 임시 식별자를 사용하기 때문에 공격자나 다른 액세스 포인트 등 제3자로부터 단말기의 식별자를 보호할 수 있다.

**【특허청구범위】****【청구항 1】**

단말기와 무선 접속을 설정하는 적어도 2개의 액세스 포인트들과 상기 단말기를 인증하는 인증서버를 포함하는 무선 근거리 네트워크에서 상기 단말기를 인증하는 방법에 있어서,

단말기가 제1 액세스 포인트와 접속하고 초기 인증을 수행할 시, 단말기가 상기 인증서버와 미리 공유하고 있는 비밀워드를 가지고 생성한 제1 비밀키를 이용하여 상기 인증서버로부터 암호 통신을 위한 제1 세션키를 수신하고, 상기 제1 액세스 포인트가 상기 인증서버와 미리 공유하고 있는 제2 비밀키를 이용하여 상기 인증서버로부터 상기 제1 세션키를 수신하는 제1 과정과,

상기 단말기가 상기 제1 액세스 포인트로부터 제2 액세스 포인트로 핸드오버하고 재인증을 수행할 시, 상기 단말기가 이전 인증시에 생성하여 상기 인증서버와 공유하고 있는 인증정보를 가지고 생성한 제3 비밀키를 이용하여 상기 인증서버로부터 암호 통신을 위한 제2 세션키를 수신하고, 상기 제2 액세스 포인트가 상기 인증서버와 미리 공유하고 있는 상기 제2 비밀키를 이용하여 상기 인증서버로부터 상기 제2 세션키를 수신하는 제2 과정을 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 2】**

제 1 항에 있어서, 상기 제1 과정은,

상기 단말기와 상기 인증서버가 미리 공유하고 있는 비밀워드를 가지고 상기 제1 비밀키를 생성하는 단계와,

상기 단말기가 다음 인증 요청시 사용하기 위한 제1 인증정보를 생성하고, 상기 제1 비밀키를 가지고 상기 제1 인증정보를 암호화하여 생성한 제1 암호화 메시지를 상기 인증서버로 전송하는 단계와,

상기 인증서버가 상기 제1 비밀키를 가지고 상기 제1 암호화 메시지를 복호하여 얻은 상기 제1 인증정보를 저장하고, 암호 통신을 위한 상기 제1 세션키를 생성하는 단계와,

상기 인증서버가 상기 제1 비밀키를 가지고 상기 제1 세션키와 상기 제1 인증정보를 암호화하여 생성한 제2 암호화 메시지를 상기 단말기로 전송하고, 상기 제1 액세스 포인트와 미리 공유하고 있는 상기 제2 비밀키를 가지고 상기 제1 세션키와 상기 제1 인증정보를 암호화하여 생성한 제3 암호화 메시지를 상기 제1 액세스 포인트로 전송하는 단계와,

상기 제1 액세스 포인트가 상기 제3 암호화 메시지를 상기 제2 비밀키를 가지고 복호하여 상기 제1 세션키를 얻고, 상기 단말기가 상기 제2 암호화 메시지를 상기 제1 비밀키를 가지고 복호하여 상기 제1 세션키를 얻는 단계와,

상기 단말기와 상기 제1 액세스 포인트가 상기 제1 세션키를 이용하여 암호 통신을 수행하는 단계를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 3】**

제 2 항에 있어서, 상기 제1 인증정보는, 상기 단말기의 임시 식별자와 다음 인증시에 사용될 비밀키를 생성하기 위한 패스워드와 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 4】**

제 3 항에 있어서, 상기 제1 암호화 메시지는, 상기 단말기의 영구 식별자와 상기 제1 인증정보를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 5】**

제 3 항에 있어서, 상기 제2 암호화 메시지는, 상기 제1 세션키와 상기 단말기의 영구 식별자와 상기 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 6】**

제 3 항에 있어서, 상기 제3 암호화 메시지는, 상기 제1 세션키와 상기 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 7】**

제 1 항에 있어서, 상기 제2 과정은,

상기 단말기와 상기 인증서버가 이전 인증시에 상기 단말기에 의해 생성된 제1 인증정보를 가지고 상기 제3 비밀키를 생성하는 단계와,

상기 단말기가 다음 인증 요청시 사용하기 위한 제2 인증정보를 생성하고, 상기 제3 비밀키를 가지고 상기 제2 인증정보를 암호화하여 생성한 제4 암호화 메시지를 상기 인증서버로 전송하는 단계와,

상기 인증서버가 상기 제3 비밀키를 가지고 상기 제4 암호화 메시지를 복호하여 얻은 상기 제2 인증정보를 저장하고, 암호 통신을 위한 상기 제2 세션키를 생성하는 단계와,

상기 인증서버가 상기 제3 비밀키를 가지고 상기 제2 세션키와 상기 인증정보를 암호화하여 생성한 제5 암호화 메시지를 상기 단말기로 전송하고, 상기 제2 액세스 포인트와 미리 공유하고 있는 상기 제2 비밀키를 가지고 상기 제1 세션키와 상기 인증정보를 암호화하여 생성한 제6 암호화 메시지를 상기 제2 액세스 포인트로 전송하는 단계와,

상기 제2 액세스 포인트가 상기 제6 암호화 메시지를 상기 제2 비밀키를 가지고 복호하여 상기 제2 세션키를 얻고, 상기 단말기가 상기 제5 암호화 메시지를 상기 제3 비밀키를 가지고 복호하여 상기 제2 세션키를 얻는 단계와,

상기 단말기와 상기 제2 액세스 포인트가 상기 제2 세션키를 이용하여 암호 통신을 수행하는 단계를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 8】**

제 7 항에 있어서, 상기 제2 인증정보는, 상기 단말기의 임시 식별자와 다음 인증시에 사용될 비밀키를 생성하기 위한 패스워드와 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 9】**

제 8 항에 있어서, 상기 제4 암호화 메시지는, 상기 단말기의 이전 임시 식별자와 상기 제2 인증정보를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 10】**

제 8 항에 있어서, 상기 제5 암호화 메시지는, 상기 제2 세션키와 상기 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 11】**

제 8 항에 있어서, 상기 제6 암호화 메시지는, 상기 제2 세션키와 상기 난수와 상기 단말기의 임시 식별자를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 12】**

단말기와 무선 접속을 설정하는 적어도 2개의 액세스 포인트들과 상기 단말기를 인증하는 인증서버를 포함하는 무선 근거리 네트워크에서 상기 단말기가 인증을 수행하는 방법에 있어서,

제 1 액세스 포인트와 접속하고 초기 인증을 수행할 시, 상기 인증서버와의 사이에 미리 공유된 비밀워드를 가지고 제1 비밀키를 생성하는 과정과,

다음 인증 요청시 사용하기 위한 제1 인증정보를 생성하고, 상기 제1 비밀키를 가지고 상기 제1 인증정보를 암호화하여 생성한 제1 암호화 메시지를 상기 인증서버로 전송하는 과정과,

상기 인증서버로부터 상기 제1 암호화 메시지에 대응하는 제2 암호화 메시지가 수신되면, 상기 제1 비밀키를 가지고 상기 제2 암호화 메시지를 복호하여 제1 세션키를 얻는 과정과,

상기 제1 세션키를 이용하여 상기 제1 액세스 포인트와 암호 통신을 수행하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 13】**

제 12 항에 있어서, 상기 제1 인증정보는, 상기 단말기의 임시 식별자와 다음 인증시에 사용될 비밀키를 생성하기 위한 패스워드와 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 14】**

제 13 항에 있어서, 상기 제1 암호화 메시지는, 상기 단말기의 영구 식별자와 상기 제1 인증정보를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 15】**

제 13 항에 있어서, 상기 제2 암호화 메시지는, 상기 난수와 상기 제1 세션키를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 16】**

제 12 항에 있어서, 상기 제1 액세스 포인트로부터 제2 액세스 포인트로 핸드오버하고 재인증을 수행할 시, 이전 인증시에 생성한 상기 제1 인증정보를 가지고 제2 비밀키를 생성하는 과정과,

다음 인증 요청시 사용하기 위한 제2 인증정보를 생성하고, 상기 제2 비밀키를 가지고 상기 제2 인증정보를 암호화하여 생성한 제3 암호화 메시지를 상기 인증서버로 전송하는 과정과,

상기 인증서버로부터 상기 제3 암호화 메시지에 대응하는 제4 암호화 메시지가 수신되면, 상기 제2 비밀키를 가지고 상기 제3 암호화 메시지를 복호하여 제2 세션키를 얻는 과정과,



상기 제2 세션키를 이용하여 상기 제2 액세스 포인트와 암호 통신을 수행하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 17】**

제 16 항에 있어서, 상기 제2 인증정보는, 상기 단말기의 임시 식별자와 다음 인증시에 사용될 비밀키를 생성하기 위한 패스워드와 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 18】**

제 17 항에 있어서, 상기 제3 암호화 메시지는, 상기 단말기의 이전 임시 식별자와 상기 제2 인증정보를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 19】**

제 17 항에 있어서, 상기 제4 암호화 메시지는, 상기 난수와 상기 제2 세션키를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 20】**

단말기와 무선 접속을 설정하는 적어도 2개의 액세스 포인트들과 상기 단말기를 인증하는 인증서버를 포함하는 무선 근거리 네트워크에서 상기 인증서버가 상기 단말기의 인증을 수행하는 방법에 있어서,

단말기가 제1 액세스 포인트와 접속하고 초기 인증을 수행할 시, 상기 단말기와의 사이에 미리 공유된 비밀워드를 가지고 제1 비밀키를 생성하는 과정과,

상기 단말기로부터 제1 암호화 메시지가 수신되면, 상기 제1 비밀키를 가지고 상기 제1 암호화 메시지를 복호하여 다음 인증시 사용하기 위한 제1 인증정보를 얻는 과정과,

상기 단말기의 암호 통신을 위한 제1 세션키를 생성하는 과정과,

상기 제1 세션키와 상기 제1 인증정보를 상기 제1 비밀키를 가지고 암호화한 제2 암호화 메시지를 생성하여 상기 단말기로 전송하는 과정과,

상기 제1 세션키와 상기 제1 인증정보를 상기 제1 액세스 포인트와의 사이에 미리 공유된 제2 비밀키를 가지고 암호화한 제3 암호화 메시지를 생성하여 상기 제1 액세스 포인트로 전송하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

#### 【청구항 21】

제 20 항에 있어서, 상기 제1 인증정보는, 상기 단말기의 임시 식별자와 다음 인증시에 사용될 비밀키를 생성하기 위한 패스워드와 난수를 포함하는 것을 특징으로 하는 상기 방법.

#### 【청구항 22】

제 21 항에 있어서, 상기 제1 암호화 메시지는, 상기 단말기의 영구 식별자와 상기 제1 인증정보를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 23】**

제 21 항에 있어서, 상기 제2 암호화 메시지는, 상기 난수와 상기 제1 세션키를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 24】**

제 21 항에 있어서, 상기 제3 암호화 메시지는, 상기 제1 세션키와 상기 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 25】**

제 20 항에 있어서, 상기 단말기가 상기 제1 액세스 포인트로부터 제2 액세스 포인트로 핸드오버하고 재인증을 수행할 시, 이전 인증시에 상기 단말기로부터 수신한 상기 제1 인증정보를 가지고 제3 비밀키를 생성하는 과정과,

상기 단말기로부터 제4 암호화 메시지가 수신되면, 상기 제3 비밀키를 가지고 상기 제4 암호화 메시지를 복호하여 다음 인증시 사용하기 위한 제2 인증정보를 얻는 과정과,

상기 단말기의 암호 통신을 위한 제2 세션키를 생성하는 과정과,

상기 제2 세션키와 상기 제2 인증정보를 상기 제3 비밀키를 가지고 암호화한 제5 암호화 메시지를 생성하여 상기 단말기로 전송하는 과정과,

상기 제2 세션키와 상기 제2 인증정보를 상기 제2 액세스 포인트와의 사이에 미리 공유된 상기 제2 비밀키를 가지고 암호화한 제6 암호화 메시지를 생성하여 상기 제2 액세스 포인트로 전송하는 과정을 더 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 26】**

제 25 항에 있어서, 상기 제2 인증정보는, 상기 단말기의 임시 식별자와 다음 인증시에 사용될 비밀키를 생성하기 위한 패스워드와 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 27】**

제 26 항에 있어서, 상기 제4 암호화 메시지는, 상기 단말기의 영구 식별자와 상기 제2 인증정보를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 28】**

제 26 항에 있어서, 상기 제5 암호화 메시지는, 상기 난수와 상기 제2 세션키를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 29】**

제 26 항에 있어서, 상기 제6 암호화 메시지는, 상기 제2 세션키와 상기 난수를 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 30】**

단말기와 무선 접속을 설정하는 액세스 포인트와 상기 단말기를 인증하는 인증서버를 포함하는 무선 근거리 네트워크에서 상기 단말기가 최초로 접속하거나 또는 핸드오버에 의해 재접속한 상기 액세스 포인트가 상기 단말기의 인증을 수행하는 방법에 있어서,

단말기와 접속하고 인증을 수행할 시 인증서버로부터 암호화 메시지를 수신하는 과정과,

상기 인증서버와의 사이에 미리 공유된 비밀키를 가지고 상기 암호화 메시지를 복호하여 상기 단말기와의 암호 통신을 위한 세션키를 얻는 과정과,

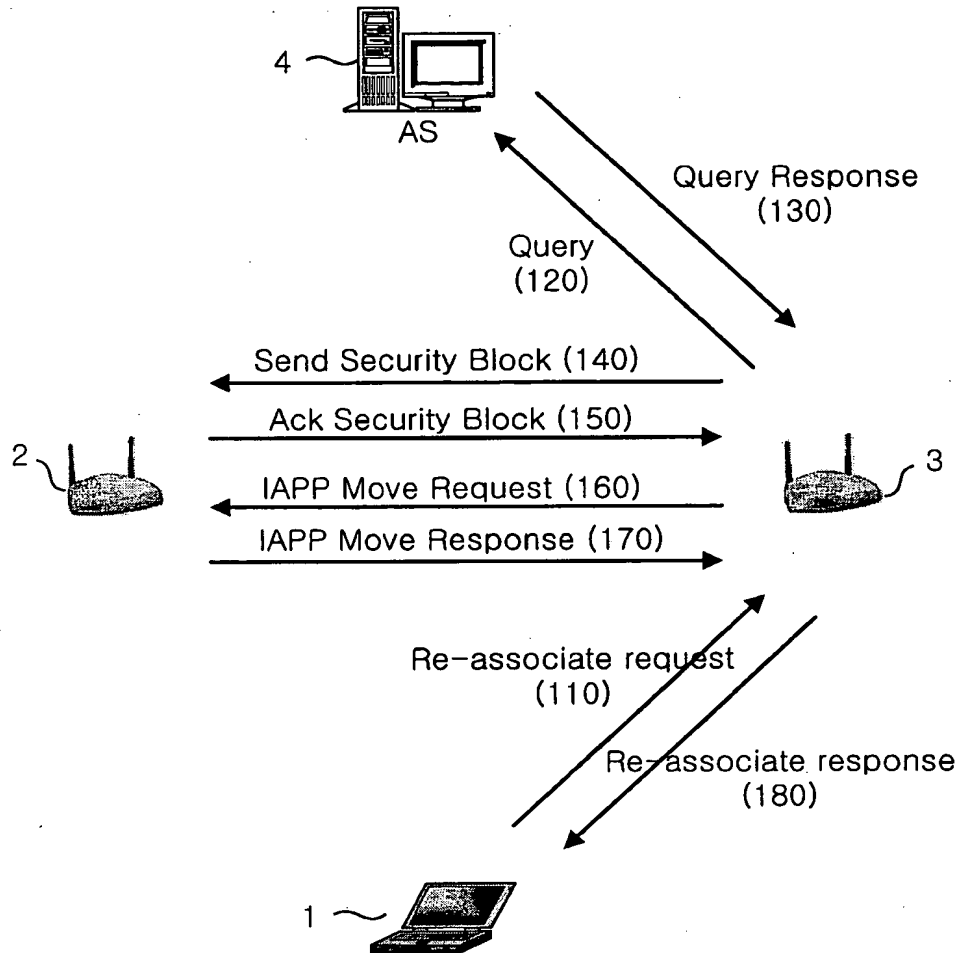
상기 세션키를 이용하여 상기 단말기와 암호 통신을 수행하는 과정을 포함하는 것을 특징으로 하는 상기 방법.

**【청구항 31】**

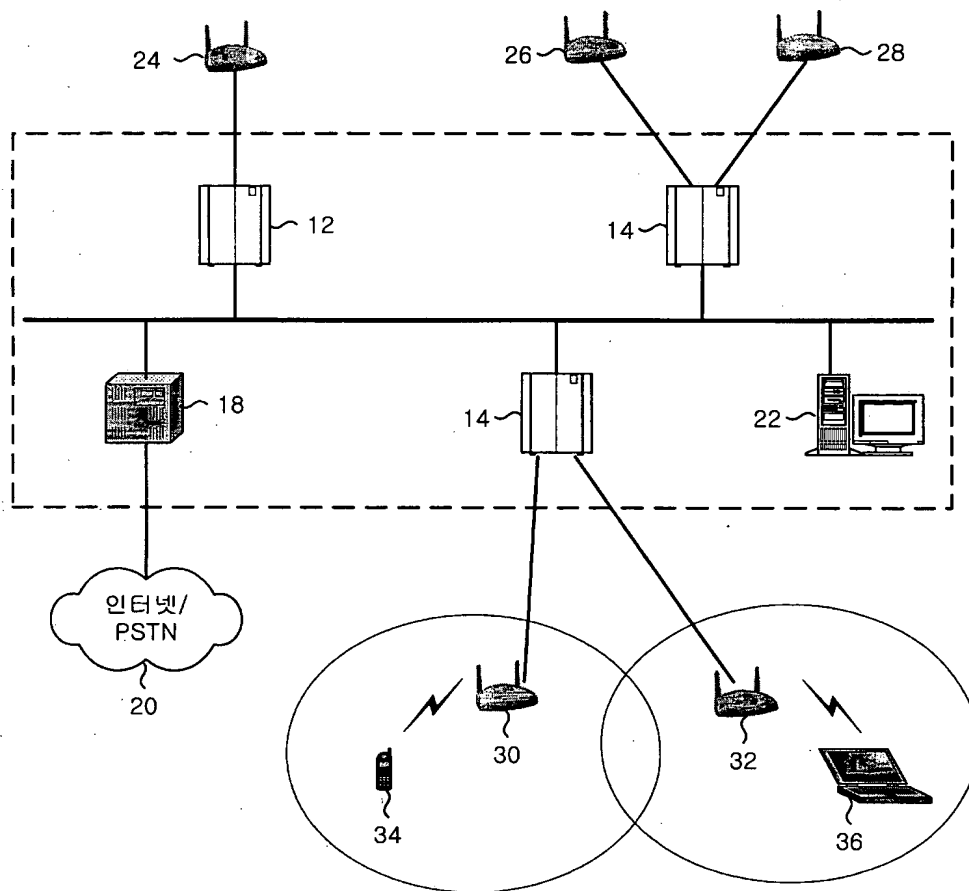
제 30 항에 있어서, 상기 암호화 메시지는, 이전 인증시에 상기 단말기에 의해 생성된 임시 식별자와 난수를 포함하는 것을 특징으로 하는 상기 방법.

## 【도면】

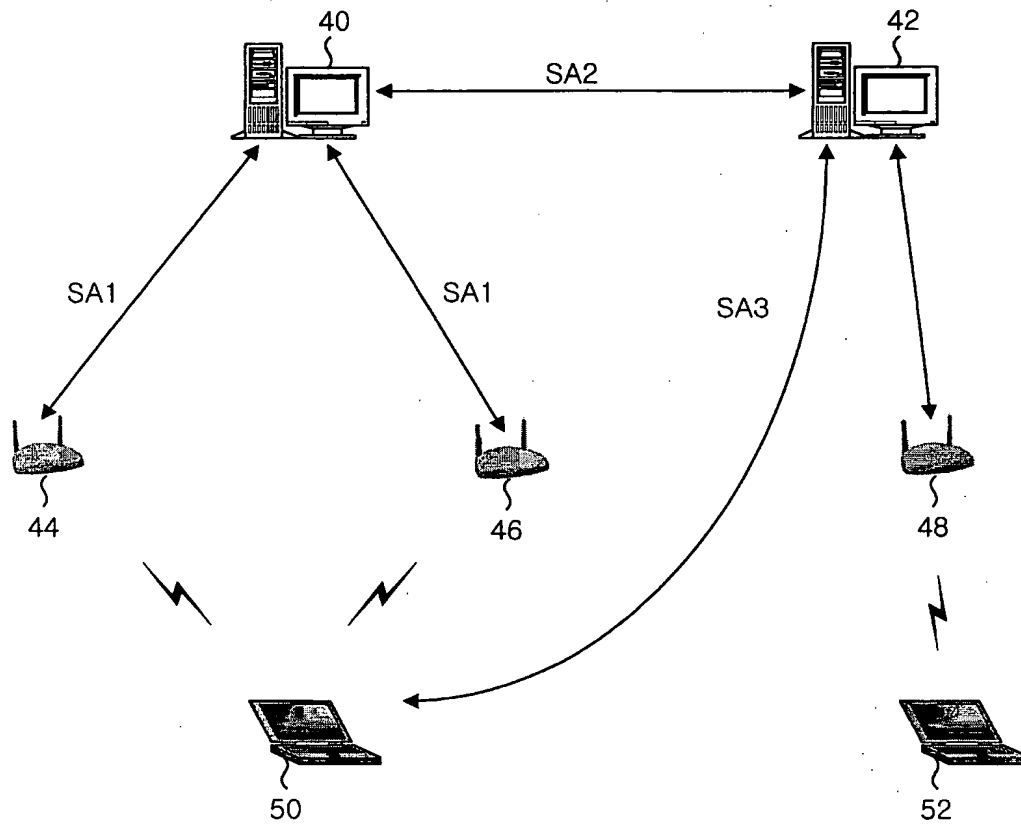
【도 1】



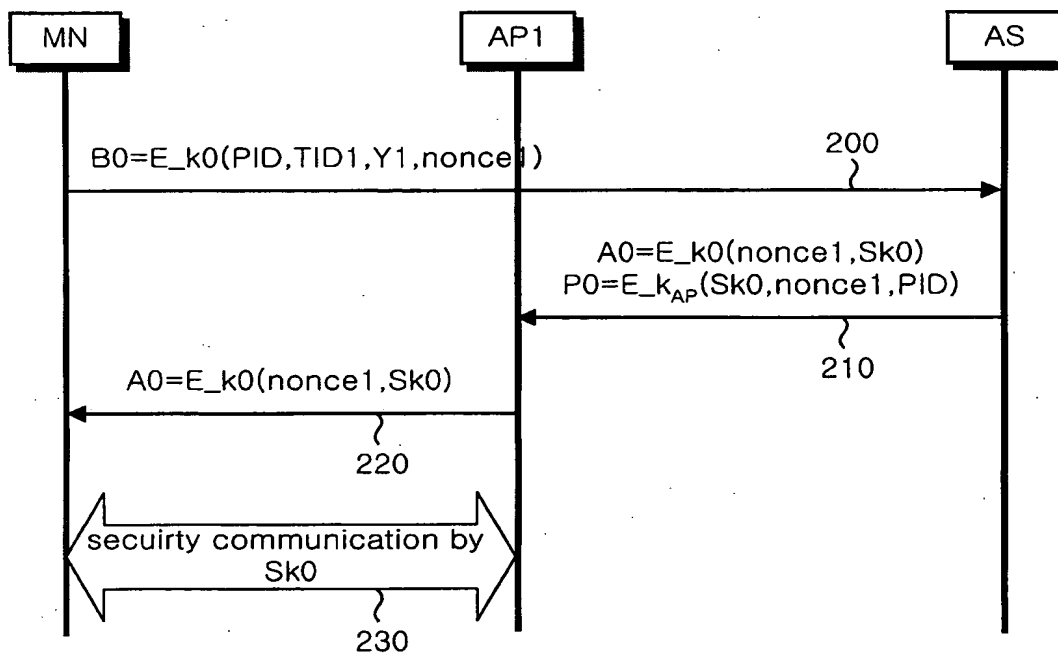
【도 2】



【도 3】

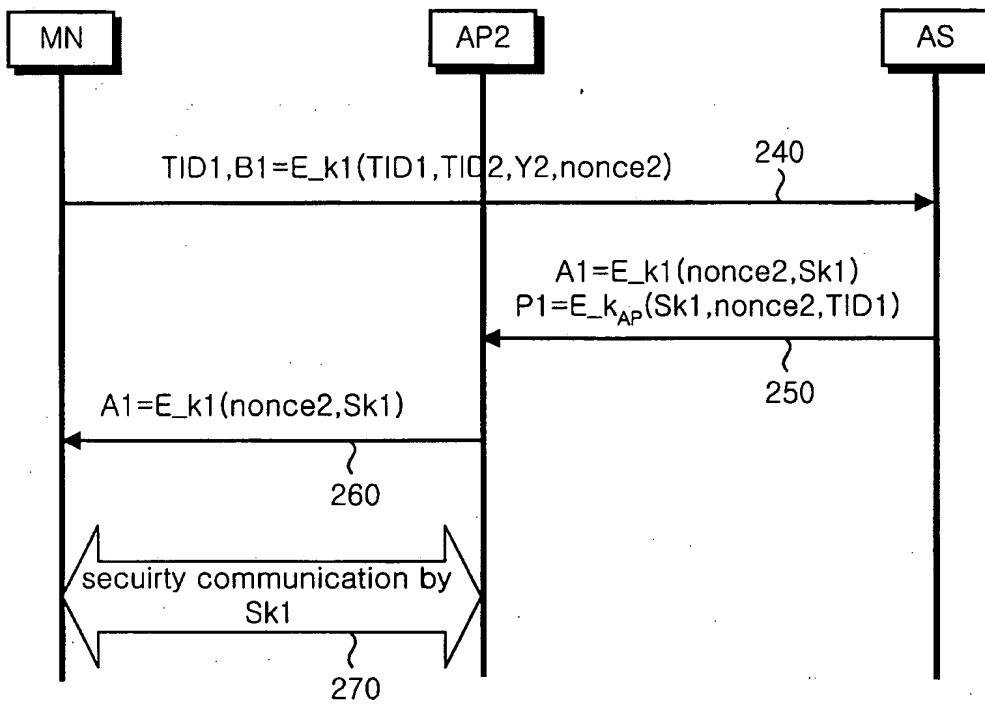


【도 4】

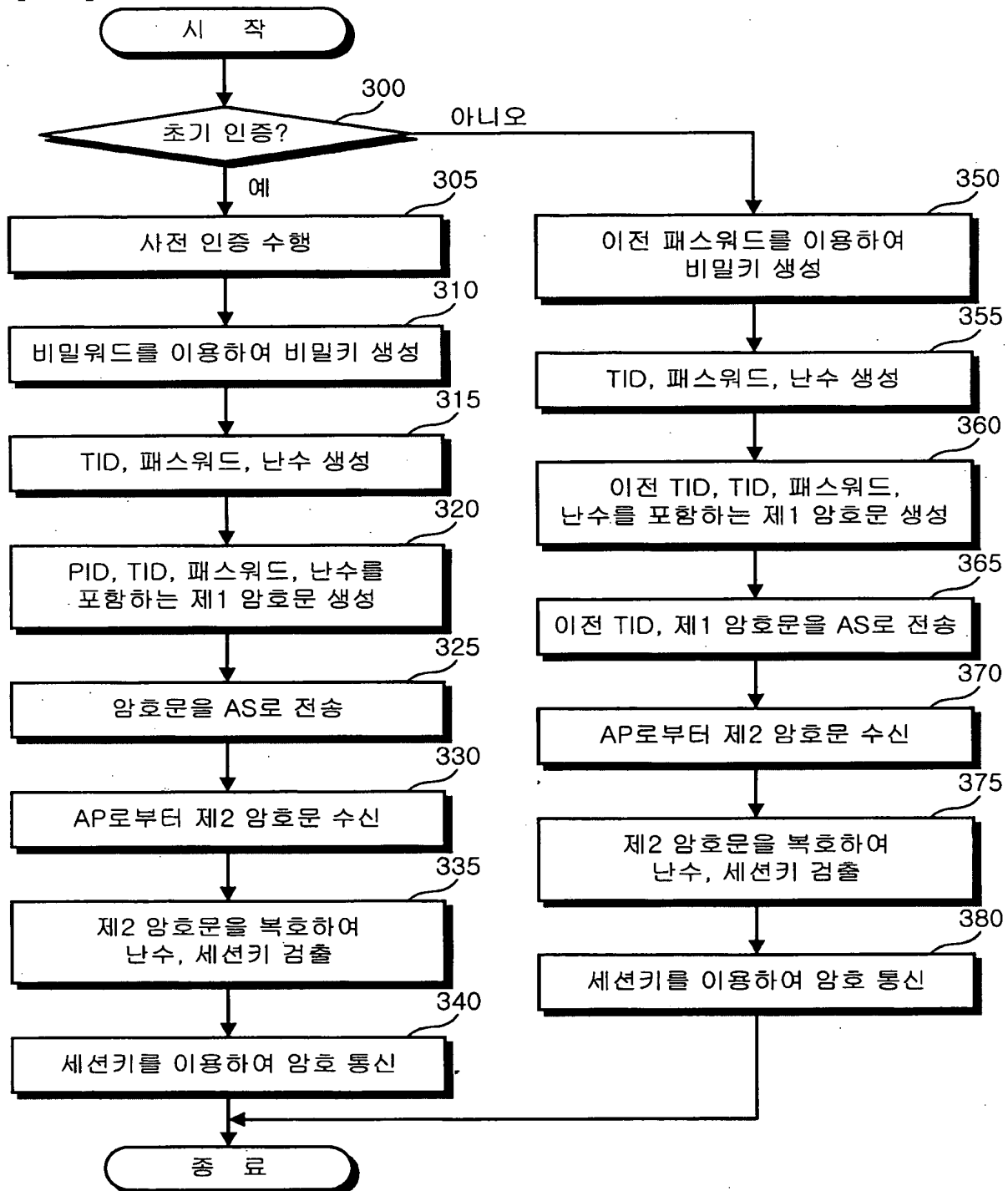




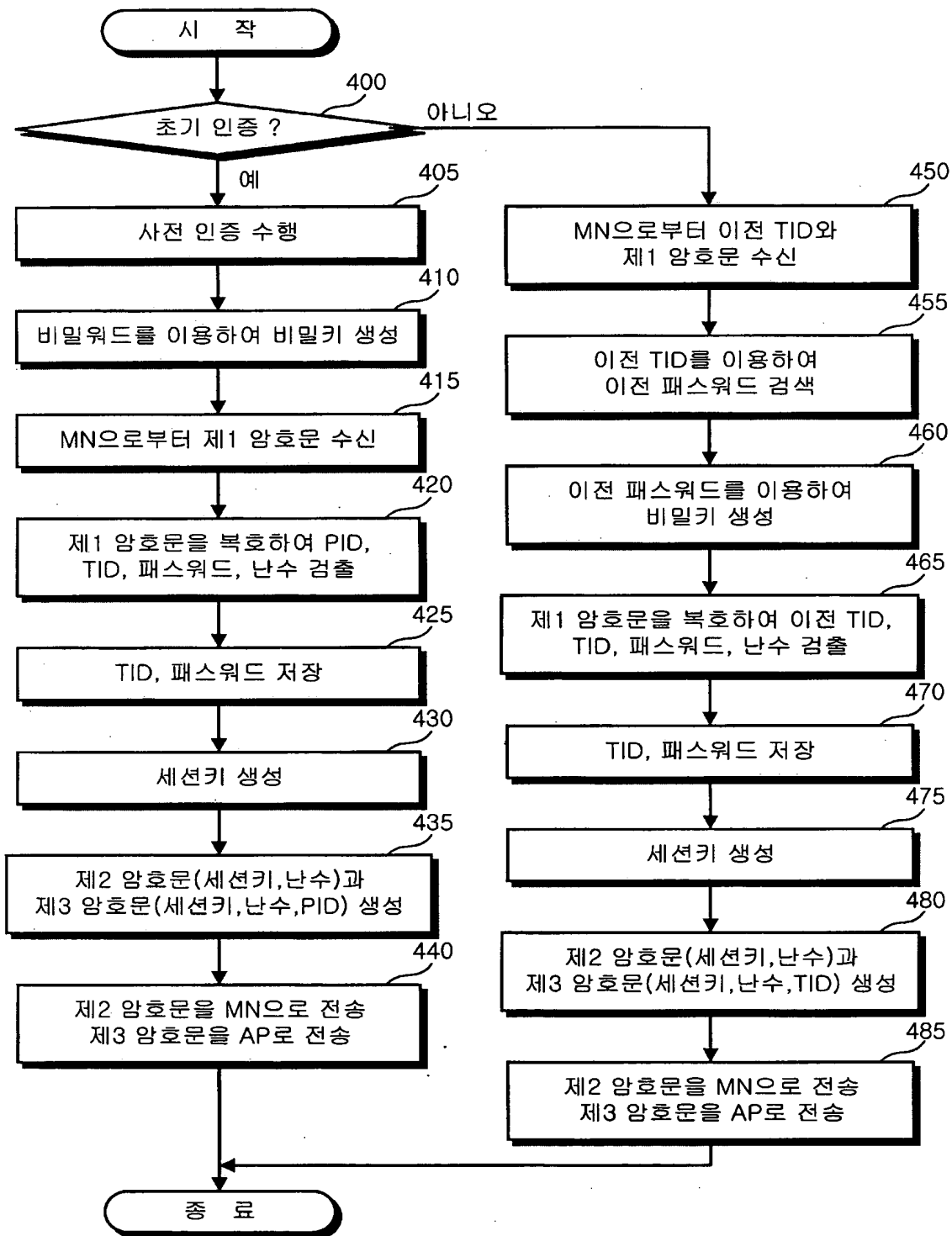
【도 5】



【도 6】



【도 7】



【도 8】

